Diffie-Hellman Key Exchange

The Diffie-Hellman algorithm is used to establish a shared secret that can be used for secret communications while exchanging data over a public network.

Diffie_Hellman key exchange works on the assumption that DDH is hard. AKA Decisional Diffie_Hellman assumption.

We say the DDH problem is hard relative to G if for all probabilistic, polynomial-time algorithms A there exists a negligible function negl, such that

$$\mathbf{Pr[A(G; q; g; gx; gy; gz) = 1] - Pr[A(G; q; g; gx; gy; gxy) = 1] \leq negl(n);}$$

where in each case the probabilities are taken over the experiment in which
G(1n) outputs (G; q; g), and then random x; y; z belonging to Zq are chosen.

DDH assumption says that cosider a cyclic group G of order q, and with generator g. The DDH assumption states that, given g ^a and g ^b for uniformly and independently chosen a, b belong to Zq. The value g ^ab looks like a random element in G.

Build Algorithm

1) Two numbers x and y are taken as input, (can be generated using some algorithm to automate the process), key, x is shared with Alice while key, y is shared with Bob.
2) Alice generates h2 with x as power in function g ^x mod q.
3) Similarly, bob generates h1 with y as power in function g ^y mod q.
4) Alice then sends h2 to Bob and Bob sends h1 to Alice.
5) Alice calculates kA as h2 ^x mod q and Bob calculates kB as h1 ^y mod q.
6) kA and kB here are same, even though the actual values were never shared through the channel.